TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ANTTI KAINULAINEN

AUTONOMISEN AJONEUVON TIETOKONENÄKÖ JA TIETOTURVAHYÖKKÄYKSILTÄ PUOLUSTAUTUMINEN

Kandidaatintyö

Tarkastaja: Pasi Hellsten

TIIVISTELMÄ

ANTTI KAINULAINEN: Autonomisen ajoneuvon tietokonenäkö ja tietoturvahyökkäyksiltä puolustautuminen
Tampereen teknillinen yliopisto
Kandidaatintyö, 30 sivua
Marraskuu 2017
Teknis-taloudellinen TkK-tutkinto-ohjelma, Tietojohtaminen
Pääaine: Teollinen liiketoiminta
Tarkastaja: Pasi Hellsten

Avainsanat: autonominen ajoneuvo, autonominen liikenne, liikenne ja logistiikka, älyliikenne, tietokonenäkö, tietoturvauhat, hyökkäykset, kirjallisuustutkimus

Itseohjautuvat ajoneuvot tekevät tuloaan kuluttajamarkkinoille, ja mukana autojen suunnittelussa ovat sekä maailman suurimmat ajoneuvovalmistajat että teknologiayhtiöt. Valmistajat kaavailevat ajoneuvojensa julkaisua vuosien 2017 ja 2022 välille, joten pian alkanee tapahtumaan mielenkiintoisia asioita autonomisten ajoneuvojen jakaessa ihmisten kanssa saman liikennejärjestelmän.

Autonomisen auton toimintaan liittyy keskeisesti erilaisten uusien ja hieman vanhempienkin teknologioiden mahdollistama tietokonenäkö, joka käytännössä sulauttaa yhteen erilaisten apulaitteiden, kuten tutkien ja videokameroiden, ympäristöstä keräämän datan. Tietokonenäkö tuo mukanaan paitsi paljon ihmissilmää tarkemman kuvan ympäristöstä, myös lukuisia tietoturvauhkia jotka ajoneuvovalmistajien on suunnittelussa otettava huomioon.

Kirjallisuuskatsauksessa käydään läpi autonomisen ajoneuvon historiaa ja lähitulevaisuuden näkymiä sekä perehdytään siihen, millaisia teknologioita ajoneuvojen tietokonenäkö käyttää hyödykseen. Tämän jälkeen esitellään tietokonenäköön liittyviä tietoturvauhkia. Tutkimuksessa havaittiin kaksi menetelmää, häiriöiden havainnointi sekä edistynyt tietokonenäön sensorifuusio, joiden avulla esiteltyihin tietoturvariskeihin voidaan varautua.

ALKUSANAT

Tämä kandidaatintyö on tehty osana tietojohtamisen koulutusohjelmaa Tampereen teknilliselle yliopistolle. Tutkimuksen aiheena ovat itseohjautuvat ajoneuvot, niiden edellyttämä tietokonenäkö sekä siihen kohdistuvilta tietoturvahyökkäyksiltä puolustautuminen. Aihe syntyi henkilökohtaisesta mielenkiinnosta autonomisia ajoneuvoja sekä liikennejärjestelmiä ja tietoturvaa kohtaan, joten aiheiden yhdistäminen tietotekniikkaa ja liikennettä käsitteleväksi kokonaisuudeksi tuntui luontevalta opintojeni historiaa ja jatkoa ajatellen.

Haluan kiittää avusta kandidaatintyöryhmääni sekä opponoijia, joiden antama palaute helpotti työn eteenpäin viemisessä. Lisäksi haluaisin kiittää ohjaajani Pasi Hellsteniä sekä vanhempiani, joiden asiantuntemus autonomisen liikenteen suhteen auttoi työn ideoinnissa ja suunnittelussa läpi syksyn.

Tampereella, 15. marraskuuta 2017.

Antti Kainulainen

SISÄLLYSLUETTELO

KESKEISET KÄSITTEET

Autonominen ajoneuvo	Autonominen ajoneuvo (engl. autonomous vehicle, self-driving car) on ajoneuvo, joka on tekoälyn ja tietokonenäön mahdollistamana kykeneväinen liikkumaan liikenteessä itsenäisesti ilman ihmiskuljettajaa (Krasniqi & Hajrizi 2016). Tunnetaan suomen kielessä myös termeillä itseohjautuva ajoneuvo tai robottiauto.
Autonominen liikennejärjestelmä	Itsestään ohjautuvista ajoneuvoista koostuva liikennejärjestelmä, jossa ajoneuvot eivät tarvitse liikkumiseen tai navigointiin erillisiä ihmiskuljettajia.
Sensorifuusio	Ajoneuvon komponenttien keräämien tietojen yhdistämistä tietokonenäöksi siten, että aikaansaatu kokonaisuus tarjoaa ympäristöstä tarkemman kuvan kuin yksikään yksittäinen komponentti (Estl 2016).
Tietokonenäkö	Tekoälyä soveltava tieteenala, joka tutkii erilaisten digitaalisten ja visuaalisten lähteiden yhdistämistä tietokoneen ymmärtämään muotoon (Ahuja 2014).
Tietoturvahyökkäys	Yritys tuhota, varastaa, muokata tai saada näkyviin hyökkääjälle kuulumatonta tietoa (International Organisation for Standardization 2016).

1. JOHDANTO

1.1 Tutkimuksen tausta ja lähtökohdat

Maailman terveysjärjestö WHO:n mukaan liikenneonnettomuuksissa kuolee maailmanlaajuisesti vuosittain noin 1,25 miljoonaa ihmistä (World Health Organization 2017). Lisäksi liikenneonnettomuudet aiheuttavat vuosittain 20-50 miljoonan ihmisen loukkaantumisen sekä yli 400 miljardin euron kustannukset (World Health Organization 2004). Yhdysvaltain liikenneministeriö julkaisi vuonna 2015 raportin, jossa tuhansien tutkittujen onnettomuuksien joukosta 94 %:ssa onnettomuuden aiheuttajaksi todettiin ihmiskuljettajan tekemä virhe (U.S. Department of Transportation 2015). Tutkimuksen mukaan ihmiset tekevät liikenteessä havainnointivirheitä, ottavat tarpeettoman suuria riskejä, käyttävät ajon aikana matkapuhelinta sekä ajavat ylinopeutta. Ihmiset pitävät liian pieniä turvavälejä, eivät käytä suuntavilkkuja, ajavat väsyneinä, raivostuvat muille tienkäyttäjille sekä ajavat humalassa. Eräänä ratkaisuna korkeaan kuolleisuuteen sekä kustannuksiin pidetään itseohjautuvia eli autonomisia ajoneuvoja (Krasniqi & Hajrizi 2016).

Autonomisella ajoneuvolla tarkoitetaan ajoneuvoa, joka on tekoälyn sekä erilaisten kameroiden ja tutkien muodostaman tietokonenäön avulla kykeneväinen liikkumaan liikenteessä itsenäisesti, liikennesäännöt ja muut tienkäyttäjät huomioon ottaen (Krasniqi & Hajrizi 2016). Ajoneuvojen automatisointi on ollut tekoälyn historian aikana yksi sen keskeisimmistä sovelluskohteista, mutta vasta viime vuosina siihen liittyvät aikaansaannokset ovat alkaneet näkymään median välityksellä tavallisille kansalaisille. Itseohjautuvuuteen liittyvää tutkimusta on kuitenkin suurten ajoneuvovalmistajien ja akateemisten laitosten toimesta tapahtunut jo vuosikymmeniä (Laugier et al. 1999).

Kymmenestä maailman suurimmasta ajoneuvovalmistajasta autonomisten autojen kehitystyöhön ovat investoineet kaikki kymmenen (Organisation Internationale des Constructeurs d'Automobiles 2016; Muoio 2017). Näiden lisäksi autonomisten autojen kehittämisessä ovat miljardiyhtiöistä mukana itsenäisesti tai ajoneuvovalmistajien kanssa yhteistyössä mm. Google, Intel, Nvidia, Apple, Uber, Microsoft sekä Samsung (CB Insights 2017). Valtaosalla autovalmistajista on edellä mainitun lähteen mukaan tavoitteena saada oma autonominen ajoneuvonsa markkinoille seuraavan viiden vuoden aikana.

Vallitsevien ennusteiden mukaan autonomiset ajoneuvot tullaan liittämään langattoman tiedonsiirron avulla osaksi suurempaa kokonaisuutta, jossa ajoneuvot ovat yhteydessä sekä toisiinsa että toistaiseksi säännöstelemättömään infrastruktuuriin (J. Petit & S. E. Shladover 2015). Toisiinsa yhteydessä olevien autonomisten ajoneuvojen muodostaman ”älyliikenteen” potentiaalisina hyötyinä pidetään onnettomuuksien ja niihin liittyvien

uhrien ja kustannusten vähenemistä, ruuhkautumisasteen madaltumista, matkustusaikojen lyhentymistä sekä tehokkaampaa teiden ja energianlähteiden hyödyntämistä (Krasniqi & Hajrizi 2016).

Tietoturvalla ja erilaisilla tietoturvahyökkäyksillä on luonnollisesti erittäin merkittävä rooli näin moniulotteisessa ja tietoon perustuvassa älyliikennejärjestelmässä, jossa ajoneuvot liikkuvat itsenäisesti koneiden muodostaman tietokonenäön avulla. Intelin ennusteen mukaan yksi autonominen ajoneuvo tulee GPS:n, kameroiden, tutkien sekä kaikuluotauslaitteiden keräämän datan johdosta käsittelemään vuonna 2020 noin 4 000 gigatavua tietoa päivässä. (Krzanich 2016) Nykyään keskivertoihminen tuottaa tietoa älylaitteillansa noin 650 megatavua päivässä, eli käytännössä yksittäinen ajoneuvo tuottaa pian saman verran dataa yhdessä päivässä kuin nykyihminen tämän päivän tottumuksillaan 17 vuodessa. Tietokonenäön vaatimien komponenttien suuri määrä sekä niiden tuottama astronominen datamassa jättävät huomattavan paljon pinta-alaa erilaisille tietokonenäön tietoturvaan liittyville hyökkäyksille ja haavoittuvuuksille, ja mahdollisesti miljoonien ihmisten henkien ollessa kyseessä tulisi autonomisen ajoneuvon tietoturvatutkimukseen ja -suunnitteluun kiinnittää erityistä huomiota.

1.2 Tutkimusongelma ja rajaus

Tutkimuksessa muodostetaan lukijalle kuva autonomisen ajoneuvon toiminnasta, sen edellyttämän tietokonenäön käyttämistä teknologioista sekä siihen liittyvistä tietoturvauhista ja -haavoittuvuuksista. Tutkimuksen tavoitteena on paitsi selvittää erilaisia keinoja autonomisen ajoneuvon tietokonenäön tietoturvan parantamiseksi, myös antaa lukijalle kattava yleiskuva ajoneuvon hyödyntämistä laitteista. Taulukossa 1 on esitelty työn päätutkimuskysymys sekä sitä tukevia alatutkimuskysymyksiä, joiden tarkoitus on auttaa kokonaiskuvan hahmottamisessa ja johdatella päätutkimuskysymyksen vastauksen äärelle.

Taulukko 1. *Pää- ja alatutkimuskysymykset*

Päätutkimuskysymys	Miten autonomisen ajoneuvon tietokonenäköön kohdistuvilta tietoturvahyökkäyksiltä voidaan puolustautua?
Alatutkimuskysymykset	Miten autonominen ajoneuvo toimii?
	Miten autonominen ajoneuvo muodostaa kuvan ympäristöstään?
	Mitä on tietoturva?
	Millaisia tietoturvauhkia tietokonenäköön kohdistuu?

Tutkimuksen ulkopuolelle rajataan erilaiset sota-, ilmailu- ja avaruusteollisuudessa käytettävät autonomiset tai kauko-ohjattavat ajoneuvot, kuten esimerkiksi miehittämättömät panssarivaunut, hävittäjät ja avaruusalukset. Näiden toiminta, toimintaympäristö sekä infrastruktuuri saattavat erota huomattavasti yleisestä liikennejärjestelmästä, joten myös niissä käytetyt ratkaisut oletettavasti eivät ole sellaisenaan sovellettavissa tutkimuksen alaiseen kontekstiin.

Tutkimuksen rakenne mukailee TTY:n opinnäytetyön mallirakennetta. Tutkimus sisältää johdannon, tutkimusmenetelmän esittelyn, kolme päälukua sekä yhteenvedon. Luvussa 2 esitellään käytetty tutkimusmenetelmä sekä kirjallinen tutkimusaineisto. Luku 3 käsittelee kolmen alaluvun avulla autonomisen ajoneuvon historiaa, itseohjautuvuuden jaottelua eri asteille sekä keskeisiä tietokonenäön mahdollistavia komponentteja ja niiden taustalla olevia teknologioita. Luvussa 4 käydään läpi tietoturvan perusteita sekä autonomisen ajoneuvon tietokonenäköön liittyviä tietoturvariskejä ja -hyökkäysmenetelmiä. Viidennessä luvussa vastataan työn päätutkimuskysymykseen esittelemällä menetelmiä tietoturvauhilta puolustautumiseen. Menetelmien tarvetta perustellaan neljännessä pääluvussa esiteltyihin tietoturvauhkiin viitaten.

2. TUTKIMUKSEN TOTEUTUS

2.1 Tutkimusmenetelmä

Kandidaatintyö toteutettiin kirjallisuustutkimuksena. Lähdemateriaalia etsittiin Tampereen teknillisen yliopiston oppilaiden ilmaisessa käytössä olevista tieteellisistä Andor- sekä Web of Science -tietokannoista. Tietokannoista löytyi useita hyviä kirjoja, tieteellisiä tutkimuksia sekä ajankohtaisia konferenssijulkaisuja aiheeseen liittyen. Aiheen ajankohtaisuuden sekä tutkimukseen liittyvien nopeasti kehittyvien teknologioiden johdosta lähdemateriaalina käytettiin myös ajankohtaisia uutisartikkeleita sekä ajoneuvojen ja niiden komponentteja valmistavien yritysten teknisiä tietopaketteja. Tieteellisten tietokantojen ulkopuolisen tiedon hyödyntämisessä käytettiin lähdekriittisyyttä, ja uutisten osalta suosittiin suuria ja kansainvälisesti tunnettuja tiede- ja talouslehtiä.

Alla olevaan taulukkoon 2 on lueteltuina keskeisimpiä työn tiedonhaussa käytettyjä hakusanoja sekä niitä vastaavat hakutulokset tietokannoittain. Tiedonhaussa hyödynnettiin Boolen operaattoreita siten, että sanan vaihtoehtoiset kirjoitusasut tulisi otettua haussa huomioon.

Taulukko 2. *Tutkimuksessa käytettyjä hakulausekkeita tietokannoittain (haut suoritettu 14.11.2017)*

Hakulauseke	Andor	Web of Science	IEEE Xplore
"autonomous vehicle" AND (cybersecurity OR "cyber security")	2 102	8	9
"autonomous vehicle" AND "computer vision"	3 608	82	188
(autonomous OR "self-driving") AND cybersecurity	5 437	15	4

Hakutulosten seasta oli helposti löydettävissä aiheeseen liittyviä teoksia järjestelemällä hakutulokset relevanssin mukaan. Etenkin työn edetessä ja aiheen tultua tutummaksi myös tiedonhausta tuli spesifimpää, ja esimerkiksi tekniikan alan tutkimusjärjestö IEEE:n tieteellisten julkaisujen tietokannasta oli helppo hakea ajankohtaista tietoa liittyen uusiin teknologioihin. Myös Google Scholar -tietokannasta oli hyötyä eri teknologioihin ja komponentteihin perehtyessä.

2.2 Tutkimusaineisto

Teosten relevanssin ja julkaisuvuoden perusteella hakutuloksista pyrittiin etsimään kandidaatintyön aiheen kannalta mahdollisimman oleellisia julkaisuja. Tutkimusaineisto rajautui vain suomeksi tai englanniksi kirjoitettuihin teoksiin, ja ydinaineisto pyrittiin pitämään alan nopean kehityksen vuoksi vuotta 2012 tuoreempana. Alla olevaan taulukkoon 3 on koottu tutkimuksen ydinaineisto, johon perehdyttiin syvästi riittävän taustatiedon takaamiseksi.

Taulukko 3. *Kirjallisuuskatsauksen ydinaineisto*

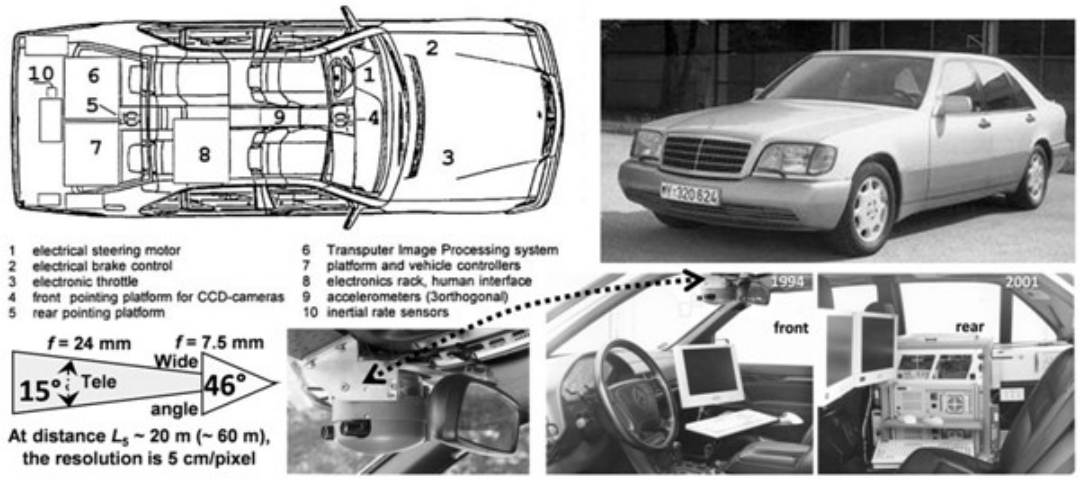
Kirjoittaja ja vuosi	Julkaisun nimi	Kuvaus
Krasniqi & Hajrizi. 2016.	Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles	Teos esittelee laajalti autonomisen liikenteen perusteita, haittoja ja hyötyjä, tulevaisuuden näkymiä sekä ajoneuvojen käyttämää teknologiaa.
Straub et al. 2017.	CyberSecurity considerations for an interconnected self-driving car system of systems	Julkaisu esittelee toisiinsa liitettyjen autonomisten ajoneuvojen muodostamaan liikennejärjestelmään kohdistuvia tietoturvariskejä, alan termistöä sekä ajoneuvojen päätöksentekomenetelmiä.
J. Petit & S. E. Shladover. 2015.	Potential Cyberattacks on Automated Vehicles	Julkaisussa käydään läpi autonomisiin ajoneuvoihin sekä tietokonenäön kannalta keskeisimpiin komponentteihin kohdistuvia tietoturvahyökkäyksiä.
Axelrod. 2017.	Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks	Julkaisussa esitellään autonomisen liikenteen erilaisia tiedonsiirtoväyliä ja -tapoja sekä niihin liittyviä tietoturvariskejä.

Yllä lueteltujen teosten lisäksi tutkimusaineistoon kuului erinäisiä uutisia mm. Forbesin, BBC:n, EE Newsin ja New York Timesin julkaisuista sekä teknisiä yksityiskohtia alan asiantuntijoiden haastatteluista, ministeriöiden nettisivuilta sekä teknologiayhtiöiden nettisivuilta.

3. AUTONOMINEN AJONEUVO

3.1 Autonomisen ajoneuvon historia ja lähitulevaisuuden näkymät

Autojen automatisointi on kiinnostanut ihmiskuntaa jo pitkään. Vuonna 1925 Yhdysvalloissa ajettiin ensimmäistä kertaa julkisella tiellä autoa, joka toimi etäohjatusti täysin ilman autossa sijaitsevaa kuljettajaa (Gora & Rüb 2016). Tietokoneet ja kehittynyt teknologia mahdollistivat ensimmäisen todella itseohjautuvan auton kehittämisen vasta 60 vuotta myöhemmin, kun 80-luvulla silloinen autovalmistaja Daimler-Benz yhdessä Münchenin yliopiston kanssa osana Prometheus-tutkimusprojektia aloitti itseohjautuvan Mercedes-Benz W140 -mallin auton suunnittelun (Oagana 2016). Projektissa tietokonenäkö saatiin aikaiseksi neljällä videokameralla, ja nykyajan älypuhelimen laskentatehoa vastaavan supertietokoneen avulla auto ajoi itsensä vuonna 1995 Münchenistä Kööpenhaminaan. Kyydissä olevat tarkkailijat joutuivat puuttumaan ajoon ainoastaan poikkeuksellisissa olosuhteissa, kuten rakennustyömaiden kohdalla. 1 700 kilometrin matkan aikana auto osasi lukea liikennemerkkejä, pitää kirjaa muista tienkäyttäjistä sekä ohittaa kanssaautoilijoita saksalaisilla moottoriteillä 185 kilometrin tuntinopeudessa. Tarkoituksena ei kuitenkaan vielä ollut rakentaa massatuotettavaa itseohjautuvaa autoa, vaan osoittaa tietokoneiden potentiaali liikenneturvallisuuden parantamisessa. Kuvassa 1 on kuvattuna kyseisen projektin kehittelemä autonominen auto sekä sen käyttämiä laitteistoja.

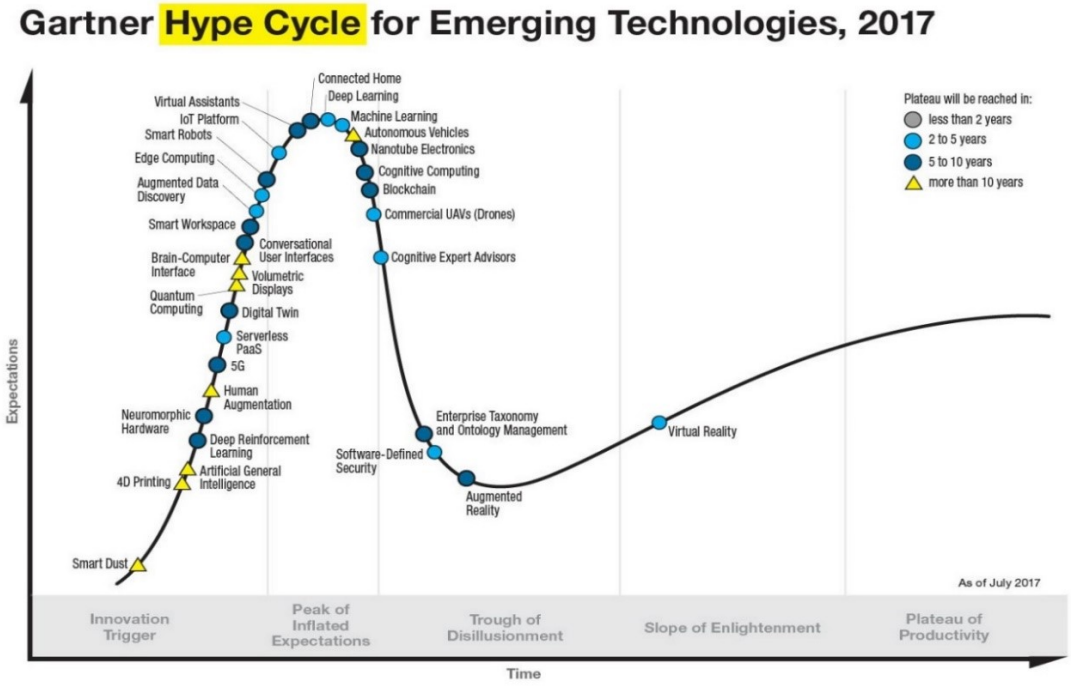


Kuva 1. *Prometheus-tutkimusprojektin aikaansaama autonominen Mercedes-Benz W140 vuodelta 1995 (Caruso 2017)*

Mitä enemmän asiaa ajattelee ajoneuvotekniikan historian näkökulmasta, sitä vähemmän yllättävänä lähitulevaisuuden autojen ohjaamisen siirtämistä tietokoneen tehtäväksi voidaan pitää. Modernit autot ovat jo valmiiksi erittäin monimutkaisia tietokoneita, jotka

toimivat yhteistyössä kymmenien pienempien tietokoneiden eli sähköisten moottorinohjausyksiköiden kanssa (BBC News 2010; Wojdyla 2012). 1970-luvulta lähtien tietokoneet ovat tutkimusten mukaan parantaneet liikenneturvallisuutta merkittävästi esimerkiksi ajonvakautus-, luistonesto- ja ABS-järjestelmien avulla (Broughton & Baughan 2002). Sähköisten teknologioiden vuoksi auto osaa pitää automaattisesti riittävää turvaväliä, varoittaa pimeässä kulmassa sijaitsevasta kanssaliikennöitsijästä, avustaa peruuttamisessa ja parkkeeraamisessa, tarkkailla kuljettajan väsymystä sekä vaihtaa kaistaa turvallisesti. Käytännössä auto koostuu jo nykypäivänä sadoista tietokoneelle ulkoistetuista ominaisuuksista, joiden ansiosta ihmisen tarvitsee vain osata painaa kaasupoljinta aktivoidakseen tietokoneohjatun polttoaineen suihkutuksen, painaa jarrupoljinta aktivoidakseen tietokoneohjatut lukkiutumattomat jarrut sekä kääntää kevyesti ohjauspyörää, jolloin sähköinen ohjaustehostin huolehtii raskaiden pyörien kääntämisestä. Ihmistä ei teknisesti tarvita edes kaasuttamiseen, jarruttamiseen tai ohjaamiseen, vaan näiden oikea-aikaiseen ajoittamiseen. Voidaankin päätellä, että autonomisen auton tuoma mullistavuus perustuu lähinnä erilaisten kohteiden reaaliaikaiseen havainnointiin tietokonenäön muodostaman kuvan avulla sekä johtopäätösten tekemiseen näiden tietojen perusteella.

ICT-alan tutkimusyhtiö Gartner lisäsi autonomiset ajoneuvot nousevien teknologioiden hype-käyrällensä ensimmäisen kerran vuonna 2010. Vuoden 2017 julkaisussa autonomiset autot ovat saavuttaneet vaiheen ”liioiteltujen odotusten huippu” (seuraavassa kuvassa englanninkielinen vaihe ”peak of inflated expectations”) (Panetta 2017). Tulevina vuosina se siirtynee vaiheeseen ”pettymyksen aallonpohja” (”trough of disillusionment”). Kuvassa 2 autonomiset autot löytyvät kyseiseltä hype-käyrältä viimeisenä keltaisena kolmiona.

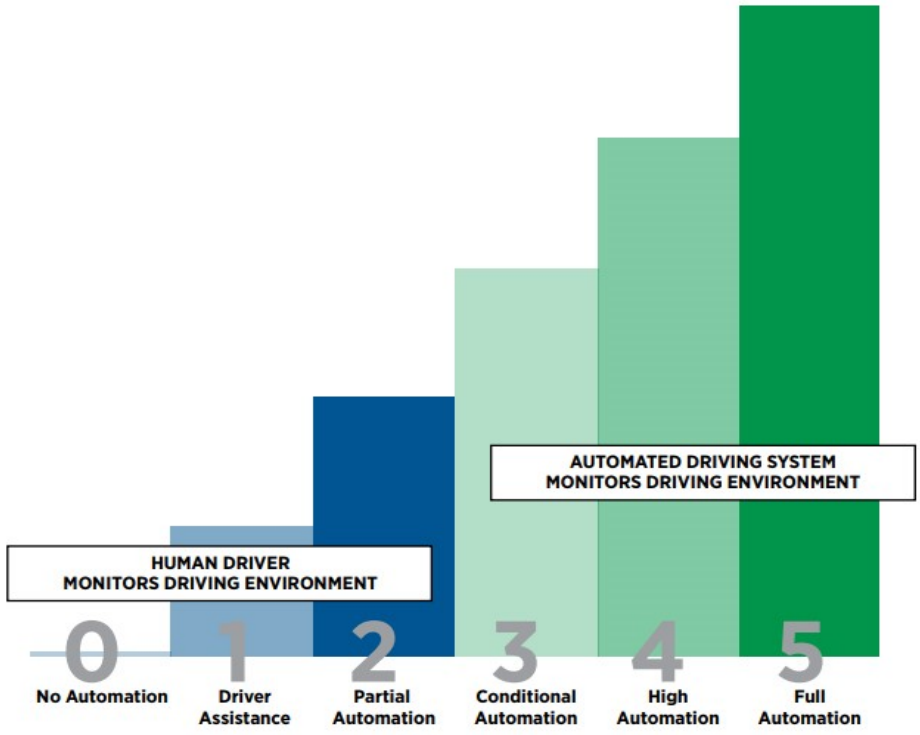


Kuva 2. *Gartnerin vuoden 2017 hype-käyrä (Panetta 2017)*

Kuvassa esitellyn hype-käyrän mukaan lähivuosina nämä vuosikymmeniä jatkuneet tutkimukset ja yritysten lupaukset konkretisoituvat kuluttajille, ja vasta laajempimittaisten käytännön kokemuksien jälkeen selviää, onko teknologialla edellytyksiä menestyä pitkällä aikavälillä. Kuvan keltaisesta kolmiosta havaitaan Gartnerin arvioineen tutkimuksessaan, että autonomisten autojen arkipäiväistymisessä ja teknologian kaupallisessa valtavirtaistumisessa kestää vielä vähintään kymmenen vuotta (Panetta 2017).

3.2 Autonomisuuden standardoidut asteet

Yhdysvaltalainen autoalan standardointijärjestö Society of Automotive Engineers julkaisi vuonna 2014 standardin, jossa itseohjautuvien ajoneuvojen automaatio on jaettu kuudelle eri tasolle automaation edistyneisyyden mukaan (Society of Automotive Engineers 2016). Standardissa automaation taso jakautuu tasaisesti eri asteille siten, että tasolla nolla automaatiota ei ole ollenkaan ja tasolla viisi auto on täysin itsenäisesti vastuussa määränpäähän pääsemisestä. Tason viisi ajoneuvossa ei täten olisi teoriassa tarvetta nykyisenkaltaisille hallintalaitteille ja esimerkiksi alaikäinen lapsi tai pyörätuolipotilas voisi käyttää autoa liikkumiseen. SAE:n standardoimat automaation tasot on omaksuttu laajalti käyttöön sekä tieteellisissä tutkimuksissa että julkisessa keskustelussa, ja usein tutkimuksen tai keskustelun ennuste kohdistuukin juuri jollekin tietylle itseohjautuvuuden tasolle tulevaisuudessa. Alla olevassa kuvassa 3 on esitelty SAE:n standardijulkaisun eri tasot.



Kuva 3. *Yhdysvaltalaisen autoalan standardointijärjestö SAE:n malli, jossa autonomiset ajoneuvot on jaettu kuudelle eri tasolle automaation edistyneisyyden mukaan (Brooke 2016)*

Standardin mukaan kolmella ensimmäisellä asteella ihmisen on jatkuvasti tarkkailtava liikennettä tavalliseen tapaan ja oltava valmiina ottamaan ajoneuvo hallintaansa. Tasolla nolla ajoneuvo saattaa hyödyntää dataa esimerkiksi varoitusten tai huomautusten esittämiseen, mutta ei auta tai puutu ajoneuvon ajamiseen tai ohjaamiseen. Ensimmäisellä tasolla automaatiota hyödynnetään ympäristöä tarkkaillen joko ohjaamiseen tai nopeuden säätelyyn, kuten esimerkiksi vakionopeudensäätimen tai kaistanvaihtoavustimen tapauksessa, mutta ei molempiin samanaikaisesti. (Society of Automotive Engineers 2016) Toisella tasolla voidaan jo puhua osittain autonomisesta ajoneuvosta, sillä auto osaa tietyissä tapauksissa itse sekä ohjata että säädellä ajoneuvon nopeutta, mutta vaatii jatkuvaa ihmisen tarkkailua.

Kolmella viimeisellä asteella autonomisuudesta alkaa olemaan mittavaa hyötyä. Tason kolme ajoneuvo osaa edetä liikenteessä automaattisesti, minkä lisäksi se myös tuntee omat rajoituksensa ja osaa varoittaa tästä kuljettajaa. Kuljettajan ei siis tarvitse tarkastella ympäristöään, mutta hänen on oltava tietyissä tapauksissa valmiina ohjaamaan autoa. Automaation edistyneisyys on tässä tapauksessa jo hyvin korkea ja ihminen voi esimerkiksi työskennellä ajoneuvon liikkuessa. Tasolla neljä ajoneuvo osaa myös reagoida itsenäisesti esimerkiksi onnettomuustilanteisiin tai poikkeaviin olosuhteisiin eikä ohjaajan tarvitse tarkkailla liikennettä tai olla valmiina ottamaan autoa hallintaansa. Neljännellä tasolla voi kuitenkin standardin mukaan olla tilanteita, joissa autonomisuutta ei voi kytkeä päälle, mutta olosuhteiden sen salliessa ei kuljettajan tarvitse kiinnittää huomiota auton toimintaan. (Hawes 2016; Society of Automotive Engineers 2016) Viidennellä tasolla kuljettajaa tai kuljettajan hallintavälineitä ei enää tarvita ja ajoneuvo osaa toimia itsenäisesti kaikissa kuviteltavissa olosuhteissa. Alla olevaan taulukkoon 4 on koottu yksityiskohtaisempi yhteenveto SAE:n standardista edellä mainittuja lähteitä mukaillen.

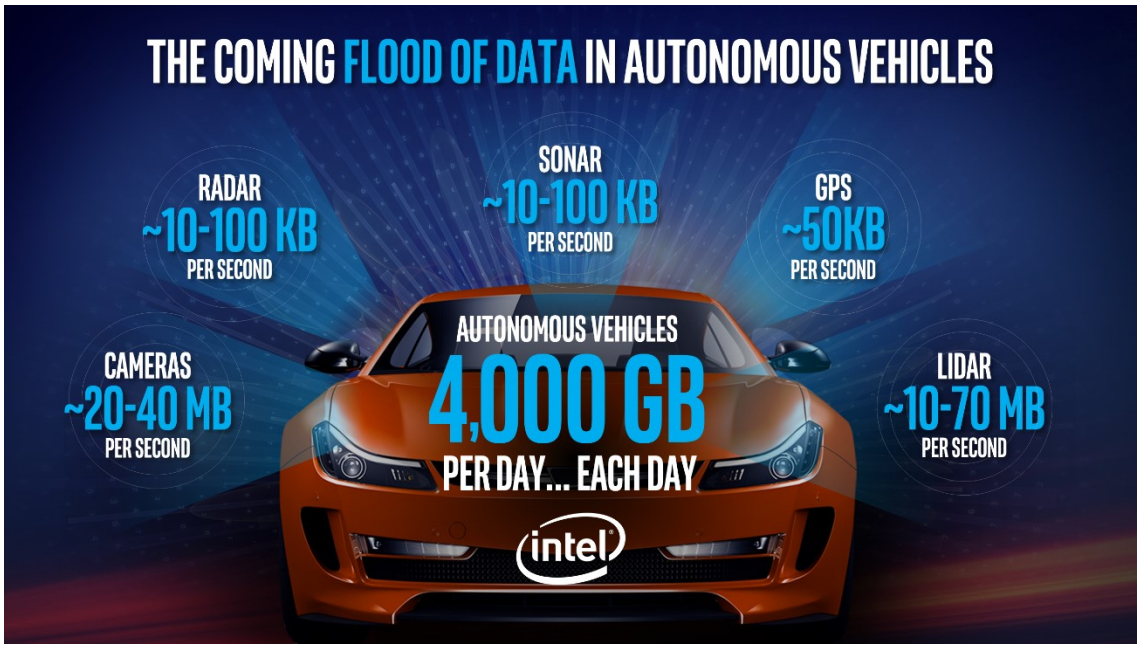
Taulukko 4. *SAE:n standardimalli autonomisten ajoneuvojen luokitteluun (mukailtu lähteistä Hawes 2016; Society of Automotive Engineers 2016)*

Taso	Autonomian edistyneisyys	Automaattinen ohjaus ja nopeuden hallinta	Kuljettajan ei tarvitse tarkkailla ympäristöä	Autonomisessa tilassa kuljettajaa ei tarvita	Autonomia olosuhteista riippumaton
0	-				
1	Avustava				
2	Osittainen	x			
3	Ehdollinen	x	x		
4	Korkea	x	x	x	
5	Täysi	x	x	x	x

Kirjoitushetkellä autonomisten ajoneuvojen tekninen kehitys etenee taulukon tasojen kaksi ja kolme välimaastossa, sillä loppuvuodesta 2017 julkaistava Audi A8 tulee yhtiön mukaan sisältämään kolmannen tason autonomiset ominaisuudet (Taylor 2017). Toisaalta autonomisuuden parissa yli kymmenen vuotta työskennellyt Ford on ilmoittanut valmistavansa vuoteen 2021 mennessä täysin ilman hallintalaitteita olevan neljännen asteen ajoneuvon, joten kehitys teknologian edistymisessä saattaa olla lähitulevaisuudessa erittäin nopeata (Belvedere 2017).

3.3 Tietokonenäön keskeiset komponentit

1980-luvun tutkimusprojekteista poiketen nykyään autonomiset ajoneuvot hyödyntävät kameroiden lisäksi tietokonenäössään lukuisia tuoreempia ja edistyneempiä teknologioita. Intelin arvion mukaan keskeisimmät komponentit auton tietokonenäön kannalta tulevat olemaan perinteinen radioaaltoihin perustuva tutka (engl. radar), lasertutka (lidar), kaikuluotain (sonar), kamerat sekä GPS (Krzanich 2016). Lisäksi useissa tutkimuksissa (mm. Petit & Shladover 2015; Joy & Gerla 2017) oletetaan ajoneuvojen hyödyntävän myös akustiikkasensoria ympärillä olevien äänten havaitsemiseen. Kuvassa 4 esitellään Intelin visio autonomisen ajoneuvon datankeruusta.



Kuva 4. *Autonomisen ajoneuvon keräämä data lähteittäin (Krzanich 2016)*

Kuvasta havaitaan, että yli 99 % kerätystä datasta tulee kameroilta ja lasertutkalta. Seuraavissa alaluvuissa on esitelty mainitut komponentit sekä niiden ominaisuuksia ja taustalla olevia teknologioita. Sijainnin aistiminen luetaan tässä työssä osaksi tietokonenäköä, sillä autonomisen ajoneuvon navigoinnin kannalta sijaintitietojen tarkka seuranta on välttämätöntä, vaikkei sijainti kirjaimellisesti olekaan osana tietokoneen ”näköä”.

3.3.1 GPS

GPS eli Global Positioning System (suom. maailmanlaajuinen paikannusjärjestelmä) on paikannusteknologia, jonka toiminta perustuu n. 20 200 kilometrin korkeudessa Maan keskikorkealla kiertoradalla sijaitseviin satelliitteihin (National Oceanic and Atmospheric Administation 2005). GPS-satelliitti lähettää Maahan atomikellolla määritellyn aikaleiman sisältävän sähkömagneettisen aallon, josta vastaanottava laite pystyy tunnetun nopeuden (valonnopeus) sekä tunnetun ajan (signaalin aikaleiman ja nykyhetken erotus) avulla laskemaan aallon kulkeman matkan eli etäisyyden satelliitilta vastaanottavalle laitteelle. Toistamalla tämän vähintään kolmella eri satelliitilla ja synkronoimalla neljännen satelliitin avulla vastaanottavan laitteen ajan samalle tarkkuudelle muiden atomikellojen kanssa, pystytään määrittelemään vastaanottavan laitteen tarkka sijainti Maan pinnalla. Autonomisen ajoneuvon suhteen teknologian toiminnan kannalta on oleellista ymmärtää, että järjestelmän atomikellot kertovat ajan 40 nanosekunnin eli sekunnin miljardisosien tarkkuudella. Tällöin sekunnin miljoonasosankin heitto kellonajoissa saattaa aiheuttaa sijaintiin kymmenien metrien epätarkkuuden Maan pinnalla.

Nykyisen GPS-järjestelmän tarkkuutta ei pidetä tarpeeksi riittävänä autonomisen liikennejärjestelmän turvallisuuden kannalta, ja SAE onkin ennustanut ajoneuvovalmistajien siirtyvän käyttämään kehitteillä olevaa kolmannen sukupolven GPS:ää vuoteen 2021 mennessä (Ashley 2016). SAE:n artikkelin mukaan kyseisellä teknologialla kohteen sijainti pystytään määrittelemään noin viiden senttimetrin tarkkuudella. GPS ei kuitenkaan yksinään ole riittävä auton sijainnin tarkkaan määrittelemiseen, sillä ympärillä olevat rakennukset tai tunnelissa ajaminen saattavat estää paikannussignaalien vastaanoton pahimmillaan pitkäksikin ajaksi. Yksi potentiaalinen ratkaisu GPS:n rinnalle tarkkojen sijaintitietojen ylläpitämiseen, olosuhteista riippumatta, esitellään seuraavaksi.

3.3.2 Inertiaalinen mittauslaite

Inertiaalisen mittauslaitteen (engl. inertial measurement unit, IMU) toiminta perustuu laitteen sisäisiin gyroskooppeihin ja kiihtyvyysantureihin, jotka yhdessä mahdollistavat ajoneuvon liikkeiden tarkan seurannan kolmiulotteisesti (OxTS 2016). GPS:n kaksiulotteisten koordinaattien sijaan inertiaalinen mittauslaite mahdollistaa nopeuden tarkan mittaamisen lisäksi myös ajoneuvon kaltevuuden ja etenemissuunnan seuraamisen. Laite ei tiedä ajoneuvon sijaintia kartalla ilman GPS-tietoja, mutta mahdollistaa sijainnin päättelemisen GPS-yhteyden katkeamisen jälkeen tapahtuneiden liikkeiden perusteella.

Paikannusteknologiaan keskittyneen isobritannialaisen laitevalmistaja OxTS:n mukaan inertiaalinen mittauslaite on autonomisissa ajoneuvoissa välttämätön apulaite liikkeen ja suunnan hahmottamisen kriittisyyden johdosta. Keulan suunnan sekä pyörimisliikkeen mittaus senttimetrien tarkkuudella on sijaintitietojen lisäksi oleellista mm. parkkeeraamistilanteessa, jolloin on laskettava reaaliajassa ajoneuvon kulmia suhteessa ympärillä oleviin autoihin (OxTS 2016).

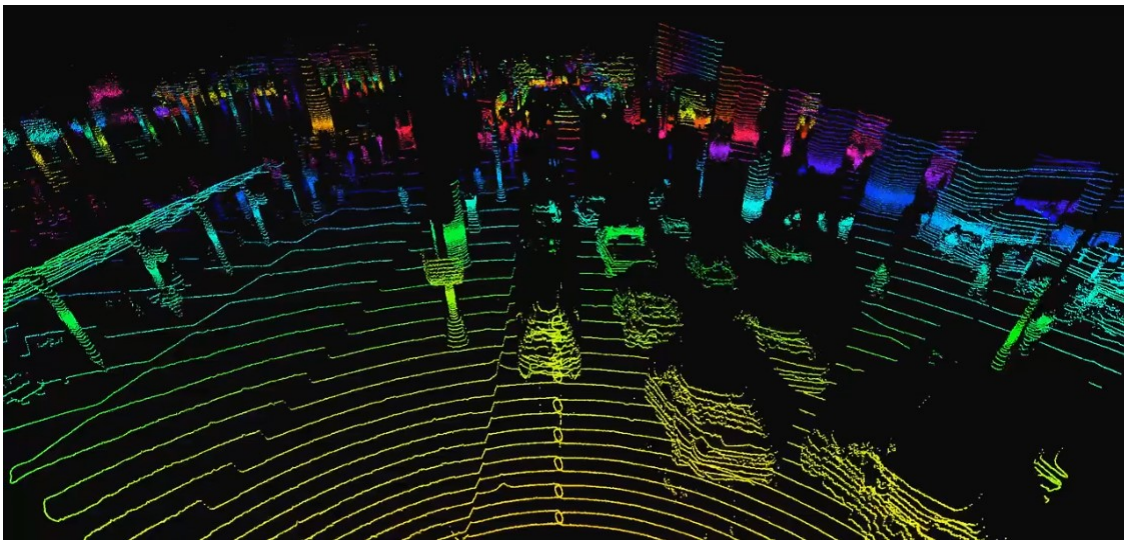
3.3.3 Tutka

Tutka (engl. radar, Radio Direction and Ranging) on toisen maailmansodan aikana kehitetty mittauslaite, joka perustuu taajuusalueen 3 Hz – 300 GHz sähkömagneettiseen säteilyyn eli tunnetummin radioaaltoihin (Bridges 2015). Tutkan radiolähetin lähettää radioaaltoja, joiden heijastumien perusteella on mahdollista tulkita radiovastaanottimen avulla kohteen sijainti, nopeus sekä etenemissuunta. 1900-luvulla tutkaa on käytetty merenkulun ja sodankäynnin lisäksi mm. sään ennustamiseen, nopeusvalvontaan sekä maanpinnan korkeuserojen kartoittamiseen.

Autonomisen ajoneuvon tapauksessa tutka on varsin hyödyllinen apuväline, sillä se mahdollistaa jopa 200 metrin päässä olevien kohteiden nopeuden ja sijainnin mittaamiseen. Lisäksi tutka on edullinen komponentti kalliimpaan lasertutkaan verrattuna, eivätkä huonot sääolosuhteet kuten sumu tai vesisade haittaa radioaaltojen kulkua (Cameron 2017). Tyypillisesti autonomiset ajoneuvot sisältävät useita, eri suuntiin suunnattuja lyhyen- ja pitkän kantaman tutkia.

3.3.4 Lasertutka

Lasertutka (engl. LiDAR, Light Detection and Ranging) on optinen tutka, joka radioaaltojen sijaan käyttää huomattavasti lyhyemmän aallonpituuden (n. 10 µm - 250 nm) laservaloa ympäristön tarkempaan kartoittamiseen. Lasertutka kehitettiin 1960-luvulla, jonka jälkeen sitä on käytetty mm. maanpinnan muotojen sekä teiden tarkkaan mallintamiseen (Cameron 2017). Autonomisten autojen tietokonenäön apuna lasertutkaa alettiin käyttämään vuonna 2005. Teknologia mahdollistaa reaaliaikaisten, muutaman senttimetrin tarkkuudella rakennettujen 360 asteen 3D-kuvien muodostamisen jopa satojen metrien päästä ajoneuvosta (Quain 2017). Kuvassa 5 esitellään tyypillinen lasertutkan muodostama, reaaliajassa päivittyvä kolmiulotteinen kuva.



Kuva 5. *Lasertutkan muodostama kuva ympäristöstä (Quain 2017)*

Kuvasta on havaittavissa, kuinka lasertutkan käyttämien lyhyen aallonpituuden valonsäteiden ansiosta on mahdollista havaita muita tienkäyttäjiä sekä jalankulkijoita satojen metrien päästä, näkyvien esteidenkin läpi. Lasertutkan heikkoutena on pidetty tuhansien tai jopa kymmenien tuhansien eurojen hinnan lisäksi sen huonoa suorituskykyä haastavissa sääolosuhteissa: usvassa sekä vesi- tai lumisateessa laitteen lähettämät valonsäteet saattavat taittua ilman pienistä hiukkasista, jolloin tutka voi tulkita ne virheellisesti kiinteiksi rakenteiksi (Bradbury 2016). Tammikuussa 2016 Ford aloitti Michiganin yliopiston kanssa lasertutkallisen autonomisen ajoneuvon testaamisen talviolosuhteissa, ja muutamaa kuukautta myöhemmin ilmoitti ratkaisseensa ohjelmistotasolla lumihiutaleiden ja sadepisaroiden erottelemisen muusta ympäristöstä lasertutkaa käytettäessä (Wong 2016). Lähteen mukaan myös muut autovalmistajat ovat testanneet ajoneuvojansa talviolosuhteissa muutamien vuosien ajan mm. Ruotsissa ja Yhdysvaltojen pohjoisessa osavaltiossa Washingtonissa, joten lasertutka kehittynee ominaisuuksiltaan paremmin käytettäväksi myös haastavammissa sääolosuhteissa.

3.3.5 Kaikuluotain

Kaikuluotain (engl. sonar, Sound Navigation and Ranging) on laite, joka hyödyntää tyypillisesti 5-50 kilohertsin taajuisia ääniaaltoja kohteen paikallistamiseksi. Luonnossa lepakot ja delfiinit ovat käyttäneet vastaavaa tapaa metsästämiseen kymmeniä miljoonia vuosia, ja ihminen oppi hyödyntämään tekniikkaa ensimmäisen maailmansodan aikaan sukellusveneiden sodankäynnissä (Cameron 2017).

Kaikuluotaus ei autonomisissa ajoneuvoissa sovellu pitkän välimatkan kohteiden paikallistamiseen, mutta ovat käteviä alle kymmenen metrin etäisyyksillä (Cameron 2017). Lyhyen välimatkan ja edullisen hinnan johdosta niitä käytetään apuna parkki- ja peruutustutkissa sekä pimeän kulman kohteiden tarkastamisessa.

3.3.6 Kamera

Autonomisissa ajoneuvoissa on tyypillisesti useita, eri suuntiin suunnattuja kameroita. Kameroiden ehdottomia etuja ovat niiden tarjoama pitkän matkan näkyvyys sekä muista tekniikoista poiketen värien, kontrastin ja tekstuurien hahmottaminen (Santo 2016). Kameroiden avulla voidaan siis lukea tiemerkintöjä, liikennemerkkejä sekä liikennevaloja, ja nähdä esimerkiksi muiden autojen jarruvalot ennen kuin tutkat huomaavat kohteen vauhdin hidastuneen jarrutuksen jälkeen. Lisäksi lämpökameroiden avulla elävien kohteiden havainnointi pimeässä helpottuu (Kite-Powell 2017). Alla olevassa kuvassa 6 on esitelty yhdysvaltalaisen Teslan valmistamissa autoissa käytössä olevan Autopilot-järjestelmän eri kameroiden tarjoamia näkymiä tieliikenteessä.

Kuva 6. *Autovalmistaja Teslan Autopilot-järjestelmän erilaisia kameranäkymiä (Tesla 2017)*

Kuvassa oikealla on näkyvissä auton käyttämiä kameroita, jotka mahdollistavat 360 asteen näkymän pisimmillään jopa 250 metrin päähän. Kuvan autossa on käytössä yhteensä kahdeksan kameraa, jotka ovat suunniteltu eri kantamille ja käyttötarkoituksiin (Tesla 2017).

3.3.7 Akustiikkasensori

Äänimaailman tarkkailu akustiikkasensorin avulla mahdollistaa tarvittaessa muiden komponenttien aistiman tiedon vahvistamisen. Tämä saattaa olla tietokonenäköön kohdistuvien tietoturvahyökkäysten tapauksessa tarpeellista tiedon oikeellisuuden takaamiseksi, mikäli eri komponentit havaitsevat ristiriitaista tietoa ympäristöstä (J. Petit & S. E. Shladover 2015).

Akustiikkasensorilla voidaan kuulla esimerkiksi lähiympäristössä olevien autojen pitämät äänet tai havaita kauempana tapahtunut liikenneonnettomuus ja sen aikaansaama äänekäs kolaus. Akustiikkasensori on autonomisessa liikenteessä lisäksi tarpeellinen hälytysajoneuvojen etäistä havainnointia varten.

3.4 Tietokonenäön tuottama kokonaiskuva

Suurten ajoneuvovalmistajien tehdessä miljardi-investointeja autonomisten autojen kehitystyöhön, ovat edellä mainitut tietokonenäössä hyödynnettävät teknologiat ottaneet massiivisia harppauksia eteenpäin viime vuosien aikana. Autot osaavat jo tällä hetkellä vaivatta tunnistaa ympäristöstä tienkäyttäjät, jalankulkijat, tiemerkinnät sekä eläimet jopa satojen metrien päässä (Tesla 2017). Tässä luvussa esitellään edellisten alalukujen

yhteenvetona grafiikkateknologiayhtiö Nvidian ratkaisu tietokonenäön muodostamiseen sensorifuusion avulla. Sensorifuusio nimensä mukaisesti sulauttaa yhteen eri sensorien keräämät tiedot ja muodostaa näiden avulla yhtenäisen ja reaaliaikaisen, tietokonenäöksi kutsutun näkymän ympäristöstä (Estl 2016). Kuvassa 7 on näkyvillä yksittäinen kuvankaappaus Nvidian järjestelmästä ajon aikana.

Kuva 7. *Grafiikkateknologiayhtiö Nvidian Drive PX -järjestelmää käyttävä itseohjautuva ajoneuvo (Nvidia 2017)*

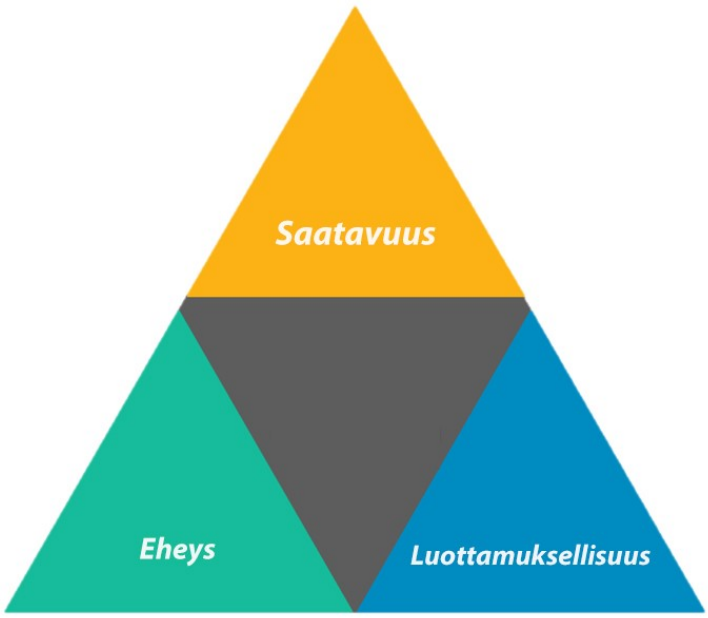
Nvidian suunnittelema Drive PX -järjestelmä on autonomisten ajoneuvojen valmistajille suunnattu syväoppivaan tekoälyyn pohjautuva tietokonejärjestelmä (Nvidia 2017). Drive PX osaa Nvidian mukaan sulauttaa yhdeksi tietokonenäöksi tutkan, lasertutkan, kaikuluotainten sekä lukuisten kameroiden datan ja muodostaa yhtenäisen 360 asteen näkymän ympäristöstä. Järjestelmä osaa myös luoda tarkkoja 3D-karttoja auton kulkemilta reiteiltä, jolloin esimerkiksi auton paikantaminen GPS-signaalin kadotessa on mahdollista aiemmin luotujen karttojen perusteella. Laskentateho järjestelmässä riittää näytönohjaimistaan tunnetun yhtiön mukaan suorittamaan noin 320 triljoonaa laskutoimitusta sekunnissa.

Autonomisen ajoneuvon tietokonenäön mahdollistavien komponenttien ei ole tarkoitus kilpailla keskenään edistyneimmän teknologian roolista, vaan täydentää toinen toisiaan (Estl 2016). Liikenneturvallisuuden ja tietokonenäön tietoturvan kannalta onkin keskeistä aistia tietoa mahdollisimman monesta lähteestä, jolloin tietoturvahyökkäyksen tapauksessa ei tarvitse tehdä äkillisiä toimenpiteitä yhden laitteen saaman datan perusteella. Seuraavassa luvussa perehdytään tietoturvan perusteiden lisäksi siihen, millaisia tietoturvariskejä edellä esiteltyjen komponenttien muodostamaan tietokonenäköön saattaa kohdistua.

4. TIETOKONENÄÖN TIETOTURVA

4.1 Tietoturva yleisesti

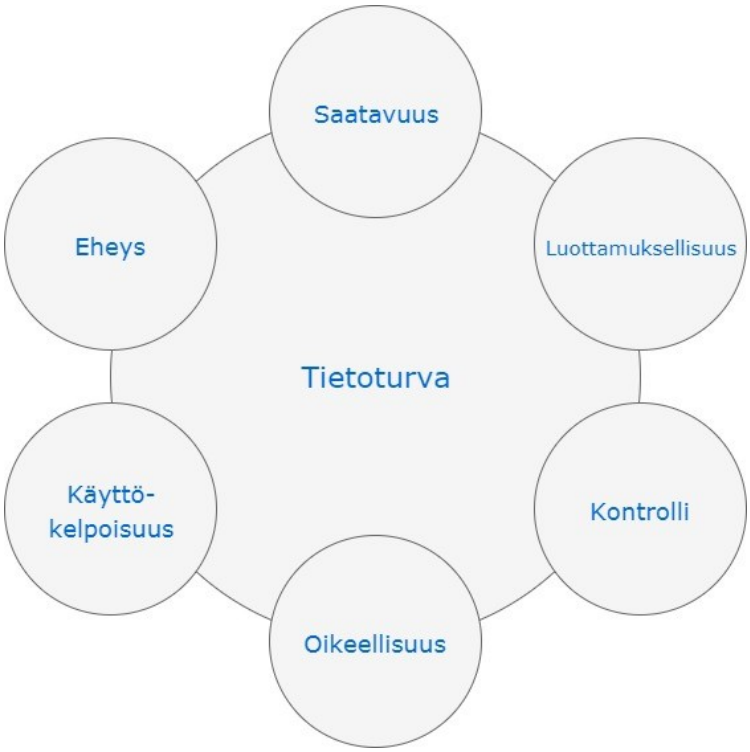
Tietoturvalla (engl. Information Security) tarkoitetaan tiedon, tietojärjestelmien ja tietoliikenteen turvaamista siten, että ulkopuolinen ei pääse näkemään, kopioimaan, muokkaamaan tai tuhoamaan hänelle kuulumatonta tietoa (Anderson 2003). Edellä mainitun lähteen mukaan yksi yleisimmistä malleista tietoturvan kuvaamiseen on niin kutsuttu CIA-malli, jossa tietoturvan hallinta jaetaan kolmeen osaan: luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Tietoturvan tavoitteena on mallin mukaisesti löytää sopiva tasapaino luottamuksellisuuden, eheyden ja saatavuuden välille, sillä liian suuri painotus yhtä ominaisuutta kohtaan saattaa merkittävästi heikentää toisia.



Kuva 8. *CIA-malli: confidentiality, integrity, availability. Mukailtu lähteestä (Anderson 2003).*

Kuvassa 8 korostuu CIA-mallin kolmiluonteisuus ja se, kuinka yhden ominaisuuden korostaminen vie fokuksen kauemmaksi muista ominaisuuksista. Esimerkiksi älypuhelimen pääsykoodina nelinumeroinen suojakoodi ei välttämättä ole kovin turvallinen, ja koodi on ulkopuoliselle helposti urkittavissa tai suhteellisen helposti arvattavissa tietokoneen avulla. Täten nelinumeroinen suojakoodi painottuisi vaivattomuutensa johdosta kolmiossa lähimmäksi ominaisuutta ”saatavuus”. Toisaalta luottamuksellisuuden nostaminen esimerkiksi merkkimäärää korottamalla laskisi huomattavasti tiedon saatavuutta, sillä koodi näppäillään kymmeniä kertoja päivittäin. Optimipisteen etsiminen on täten tapauskohtaista.

Autonomisen ajoneuvon tietoturvan tapauksessa klassinen CIA-malli on kuitenkin turhan yksiulotteinen. Tarkemman mielikuvan tietoturvasta saa aikaan lähteessä Reid & Gilbert (2010) esitellyllä niin kutsutulla Parkerin kuusikolla, joka ottaa huomioon lisäksi tiedon kontrolloinnin (control), oikeellisuuden (authenticity) sekä käyttökelpoisuuden (utility).



Kuva 9. *Tietoturva ja sen kriittiset osa-alueet Parkerin kuusikon mukaan (mukailtu lähteestä Reid & Gilbert 2010)*

Kontrollilla tarkoitetaan sitä, että tiedon saatavuuden lisäksi huomioidaan erilaiset seuraukset, joita tiedon menettämisellä tai tuhoutumisella saattaisi olla (Reid & Gilbert 2010). Autonomisen liikenteen toimivuuden kannalta saattaisi esimerkiksi olla oleellista, että julkiset navigointiin käytettävät kartat eivät missään tapauksessa pääse tuhoutumaan, mutta järjestelmän on osattava varautua myös tällaiseen tilanteeseen. Oikeellisuus kuvaa tiedon pitkäaikaisen paikkansapitävyyden ylläpitoa, eli eri tahojen järjestelmään tekemien muutosten jatkuvaa tarkkailua. Käyttökelpoisuuden tehtävänä taas on varmistaa, että tieto on käytettävissä myös tulevaisuuden tietokoneilla tai käyttöjärjestelmillä: esimerkiksi vuosikymmeniä sitten luotuun tietoon on edelleen päästävä käsiksi myös moderneilla ja lähitulevaisuuden laitteistoilla. Autonomisen ajoneuvon tietokonenäköön kohdistuvien tietoturvahyökkäysten kannalta keskeisimpiä ”suojeltavia” elementtejä Parkerin kuusikon avulla esiteltyinä ovat tiedon saatavuus, eheys, kontrolli sekä oikeellisuus.

4.2 Tietoturvahyökkäys

Tietoturvastandardi ISO-27000:n mukaan tietoturvahyökkäys tarkoittaa yritystä tuhota, varastaa, muokata tai saada näkyviin hyökkääjälle kuulumatonta tietoa (International Organiation for Standardization 2016). Tietoturvahyökkäyksen motiivina on tyypillisesti taloudellinen hyöty, terrorismi tai tietojärjestelmien haavoittuvuuden osoittaminen ja julkisen keskustelun herättäminen tietoturvan suhteen (Mozur et al. 2017). Tietoturvahyökkäyksiä tapahtuu lisäksi myös valtiollisella tasolla osana kybertiedustelua tai -sodankäyntiä, jolloin tämän tutkimuksen kontekstin kannalta vastapuolen liikenne tai liikenneinfrastruktuuri ajoneuvoineen saattaisi olla yksi mahdollisista hyökkäyksen kohteista.

Toistaiseksi autonomisiin ajoneuvoihin tai niiden tietokonenäköön kohdistuneet vähäiset tietoturvahyökkäykset ovat olleet rauhanomaisia sekä keskustelun herättämiseen pyrkiviä. Vuonna 2016 Kiinassa toteutettiin tutkimusmielessä tietoturvahyökkäys Teslan Model S -autoon, jolloin hallituissa olosuhteissa ajoneuvon jarruja, ovien lukituksia ja muita sähkölaitteita onnistuttiin hallitsemaan etänä yli kymmenen kilometrin etäisyydeltä (Solon 2016). Tutkimuksen tarkoituksena oli etsiä ajoneuvosta haavoittuvuuksia, demonstroida niitä hallitusti ja sen jälkeen raportoida haavoittuvuudet valmistajalle paikkaamista varten. Tietokonenäköön ja sen käyttämiin komponentteihin on tutkimusolosuhteissa demonstroitu tietoturvahyökkäyksiä mm. lähteessä Hocheol et al. 2017, joka esitellään osana seuraavaa lukua. Tapauksista on tutkimusolosuhteista huolimatta kuitenkin havaittavissa erilaisten hyökkäysmenetelmien suuri potentiaali, sillä esimerkiksi jarrujen lukkiutumisella moottoritiellä saattaisi olla tuhoisia seurauksia matkustajille ja muille tienkäyttäjille.

4.3 Tietokonenäköön kohdistuvia hyökkäysmenetelmiä

Alla olevaan taulukkoon 5 on kerätty IEEE:n tieteellisissä julkaisuissa esiintyviä hyökkäysmenetelmiä, joita pidetään edellisessä luvussa esiteltyjen teknologioiden ja niiden muodostaman tietokonenäön toiminnan kannalta merkittävimpinä tietoturvariskeinä. Lisäksi menetelmiin on haettu tilannekohtaisten lähteiden avulla tarkempi tekninen kuvaus tai esimerkkitapaus liittyen laitteistoon sekä riskin toimintaperiaatteeseen. Tilanteet ovat poimittu seuraavista vuosina 2015-2017 julkaistuista tutkimuksista:

- Potential Cyberattacks on Automated Vehicles (J. Petit & S. E. Shladover 2015)
- Internet of Vehicles and Autonomous Connected Car – Privacy and Security Issues (Joy & Gerla 2017)
- A Study on Cyber-Security of Autonomous and Unmanned Vehicles (Yağdereli et al. 2015)

Taulukko 5. *Autonomisen ajoneuvon tietokonenäköön kohdistuvia tietoturvauhkia*

Kohde	Menetelmä	Kuvaus ja seuraus
GPS	Häirintä	Muutaman kymmenen euron hintainen GPS-häirintälaite pystyy lähettämään ympäristöönsä satunnaissignaalia samalla taajuudella, jolla GPS-satelliitit lähettävät tietoa avaruudesta Maahan (Hu & Wei 2009). Seurauksena ajoneuvon GPS-vastaanotin on kelvoton häirinnän aikana.
	Tietoliikenteen väärentäminen	GPS-vastaanottimelle on mahdollista lähettää väärennettyjä signaaleita, joiden erottaminen autenttisen GPS-satelliitin lähettämistä signaaleista on haastavaa (University of Texas 2013). Seurauksena vastaanotin antaa ajoneuvolle väärän paikkatiedon, ja riittämättömällä tietoturvasuunnitelulla varustettu maantiellä kulkeva ajoneuvo saattaisi päätellä olevansa esimerkiksi moottoritiellä ja aiheuttaa onnettomuuden.
Kamera	Häirintä	Videokameran CCD-kennolle voidaan lähettää kirkkaita, eri intensiteettisiä valkoisia valonsäteitä, jotka saavat kameran videokuvan käyttökelvottomaksi (Greene 2006). Seurauksena ajoneuvo ei pysty hyödyntämään konenäössään kyseistä, häirinnän kohteeksi joutunutta videokameraa.
Tutka	Mekaaninen häirintä	Radioaaltoihin perustuvan tutkan häiritsemiseen on kehitetty lukuisia mekaanisia menetelmiä jo toisen maailmansodan aikana. Tutka voidaan saada havaitsemaan olemattomia kohteita sirottelemalla aidon kohteen päälle ”silpuksi” kutsuttua ainetta, joka aiheuttaa tavallista voimakkaamman vastakaiun radiovastaanottimelle (Meikle 2008, s. 107). Seurauksena ajoneuvo saattaa esimerkiksi tehdä hätäjarrutuksen, vaikka tutkan välittömässä läheisyydessä ei olisikaan aitoja kohteita.
	Elektroninen häirintä	Tutkaa on mahdollista häiritä myös lukuisin elektronisin menetelmin. Tutka voidaan tehdä käyttökelvottomaksi häirintälaitteella, joka lähettää tutkalle korkeaenergisiä signaaleja eri taajuuksilla. Toinen häirintätapa on kaapata tutkan lähettämät alkuperäiset signaalit ja toistaa ne myöhemmin uudelleen (Mahafza 1998, s. 71). Seurauksena tutka on käyttökelvoton, ja saattaa havaita epätodellisia kohteita.
Lasertutka	Häirintä	Vuonna 2017 Etelä-Korean Daejeonin teknillisessä yliopistossa tutkijat onnistuivat lasertutkan sokaisemisen lisäksi saamaan tutkan havaitsemaan epätodellisia kohteita (Hocheol et al. 2017). Tutkimuksessa sokaisuun riitti kirkkaan, vastaavan aallonpituuden valon osoittaminen tutkaa kohti. Väärennetyn kohteen luomisen tekninen toteutus liittyi vain tietynmalliseen lasertutkaan, joten sitä ei voida pitää pätevänä kaikkien lasertutkien kohdalla. Menetelmästä riippuen lasertutka oli ajoneuvolle käyttökelvoton tai havaitsi epätodellisia kohteita.

Akustiikkasensori	Häirintä	Akustiikkasensoria voidaan häiritä luomalla taustakohinaa taajuuksilla, joita ihmisen korva ei välttämättä kuule (Roy et al. 2017). Seurauksena esimerkiksi ympärillä olevien autojen äänten havainnointi on ajoneuvolle mahdotonta tai haastavaa.
	Äänimaailman jäljittely	Akustiikkasensoria on mahdollista hämätä jäljittelemällä ääntä, jonka havaitsemisesta autonominen ajoneuvo on ohjelmoitu tekemään toimenpiteitä (J. Petit & S. E. Shladover 2015). Mikäli ajoneuvo olisi esimerkiksi ohjelmoitu tekemään hätäjarrutus havaitessaan törmäyksen äänen tarpeeksi lähellä, saattaisi väärennetyn äänen toistaminen aiheuttaa vaaratilanteita.
Kaikuluotain	Häirintä	Kaikuluotaimelta voidaan piiloutua peittämällä kohde materiaalilla, josta ääniaallot eivät heijastu takaisin vastaanottimelle. Esimerkiksi Teslan Autopilot-järjestelmän kaikuluotaimelta on mahdollista piiloutua kääriytymällä materiaaliin, joka on tarkoitettu akustiikassa resonanssin vähentämiseen (Fox-Brewster 2016). Materiaali absorboi ääniaallot, jonka seurauksena kaikuluotain ei havaitse välittömässä läheisyydessä olevia kohteita ympäristössä.

Taulukosta huomataan, että lähes kaikki autonomisen ajoneuvon tietokonenäön käyttämät komponentit sisältävät teknologian luonteeseen perustuvia heikkouksia tietoturvan suhteen. Huomionarvoista on myös, että tilanne ei välttämättä vaadi aina aktiivista hyökkääjää, vaan myös kahden tai useamman laitteen lähettämät signaalit saattavat häiritä toinen toistaan. IEEE:n julkaiseman tutkimuksen mukaan esimerkiksi modernien lasertutkien suhteen ei osata vielä sanoa varmaksi, voisivatko kymmenien tai satojen lähekkäisten lasertutkien sähkömagneettiset aallot interferoida toistensa kanssa siten, että toimintaan tulisi häiriöitä (Kim et al. 2015). Autonomisia ajoneuvoja ja niiden komponenttien tietoturvaa suunnitellessa tulisi varautua paitsi teknologioiden luontaisten heikkouksien varalle, myös erilaisiin aktiivisiin tietoturvahyökkäyksiin. Seuraavassa kappaleessa käsitellään kahta menetelmää, joiden avulla ajoneuvoa voidaan suojata edellä käsiteltyjen tietokonenäköön liittyvien tietoturvahyökkäysten varalta.

5. MENETELMÄT HYÖKKÄYKSILTÄ SUOJAUTUMISEEN

Tässä luvussa perehdytään siihen, millaisin menetelmin taulukossa 5 luetelluilta tietokonenäköön liittyviltä tietoturvahyökkäyksiltä voidaan pyrkiä suojautumaan. Esitellyt suojautumismenetelmät ovat ajoneuvoon kohdistuvan ulkopuolisen hyökkäyksen tai häiriön havainnointi sekä edistynyt sensorifuusio. Menetelmien tarvetta kuvataan lähteessä J. Petit & S.E. Shladover (2015), jonka lisäksi tarvetta edistyneelle sensorifuusiolle kuvataan mm. lähteissä Straub et al. (2017) sekä Axelrod (2017).

5.1 Hyökkäyksen havainnointi

Erilaisten häiriönestolaitteiden (engl. anti-jamming device) avulla on tietyissä määrin mahdollista suojata ajoneuvon joitakin komponentteja ulkopuolisilta hyökkäyksiltä, mutta käytettyjen teknologioiden luontaisten heikkouksien johdosta häiriönestolaitteiden toteuttaminen ei esimerkiksi kameroille tai lasertutkille ole toistaiseksi mahdollista (Chien 2015). Sen sijaan hyökkäyksen tunnistaminen ja asianmukaiset toimenpiteet ovat helpommin toteutettavissa ohjelmistopuolella: mikäli jonkin komponentin syötteessä havaitaan häiriötä tai sen käyttö estyy hyökkäyksen vuoksi kokonaan, tulisi ajoneuvon turvautua toisten sensoreiden tarjoamaan dataan (J. Petit & S. E. Shladover 2015). Edellä mainitun lähteen esimerkkiennusteissa yli puolet mahdollisista komponentteihin kohdistuvista hyökkäystilanteista ovat mitätöitävissä toisten komponenttien havainnoimaa dataa hyödyntämällä, josta voidaankin päätellä hyökkäyksen havainnoinnin ja tämän perusteella vaihtoehtoisten tietolähteiden hyödyntämisen olevan hyvin keskeistä hyökkäyksiltä puolustautuessa.

IEEE:n julkaiseman tutkimuksen mukaan GPS:n kohdistuva häirintä on mahdollista tunnistaa lähes välittömästi häirinnän alettua (Zhang et al. 2012). Kameran tai lasertutkan tapauksessa hyökkääjän käyttämän kirkkaan valon havaitseminen tulisi ohjelmistopuolella olla merkki siitä, että kyseiseen laitteeseen saattaa kohdistua hyökkäys ja datan käyttäminen ajoneuvon päätöksentekoon on täten riskialtista. Tutkan, akustiikkasensoriin tai kaikuluotaimeen kohdistuva hyökkäys on mahdollista havaita käyttämällä ajoneuvon kameroita tai lasertutkaa ympäristön kohteiden tarkistamiseen ennen mahdollisia toimenpiteitä.

Yksittäisten komponenttien laajan hyökkäyspinta-alan johdosta ympäristön tarkkailu on viisasta toteuttaa mahdollisimman monen teknologian avulla: esimerkiksi lasertutka saattaa olla hyödyllisin yksittäinen komponentti ympäristön tarkkailussa, mutta mikäli siihen kohdistuvan häiriön vuoksi se ei ole tilapäisesti käytettävissä, pystyy auto navigoimaan myös pelkästään kameroiden ja tutkien avulla ja kytkemään lasertutkan tilapäisesti pois

käytöstä. Tästä on käytännön esimerkkinä Teslan Autopilot-toiminto, joka ei ainakaan toistaiseksi käytä navigoinnissaan olleenkaan lasertutkaa (Tesla 2017). Häiriöiden havaitsemisen lisäksi autonomisen ajoneuvon tulisi osata tehdä toimenpiteitä häiriöiden korjaamiseksi: tähän tarvitaan seuraavaksi esiteltävää menetelmää eli edistynyttä sensorifuusiota.

5.2 Edistynyt sensorifuusio

Sensorifuusiolla tarkoitetaan ajoneuvon komponenttien keräämien tietojen yhdistämistä tietokonenäöksi siten, että aikaansaatu kokonaisuus tarjoaa ympäristöstä tarkemman kuvan kuin yksikään yksittäinen komponentti (Estl 2016). Pohjimmillaan tarkoituksena on hyödyntää eri teknologioiden tarjoamat parhaat puolet, sekä paikata niiden heikkouksia muiden komponenttien avulla. Komponenttien runsas määrä paitsi tarkentaa ajoneuvon saamaa kuvaa ympäristöstä, myös mahdollistaa erilaisten vaihtoehtoisten teknologioiden hyödyntämisen, mikäli ajoneuvon tietokonenäkö joutuu onnistuneen tietoturvahyökkäyksen kohteeksi. Alla olevaan taulukkoon 6 on hahmoteltu vaihtoehtoisia tapoja selvitä tietoturvahyökkäyksestä sensorifuusion avulla, mikäli kyseessä on hyökkäys yksittäistä komponenttia kohtaan (J. Petit & S. E. Shladover 2015; Estl 2016).

Taulukko 6. *Vaihtoehtoisia tapoja havainnoida ympäristöä autonomisen ajoneuvon tietokonenäön yksittäisen komponentin joutuessa tietoturvahyökkäyksen kohteeksi*

Hyökkäyksen alainen komponentti	**Vaihtoehtoiset komponentit**
GPS	Inertiaalinen mittauslaite, 3D-kartat
Tutka	Lasertutka, kamerat, kaikuluotaimet
Lasertutka	Kamerat, tutkat, kaikuluotaimet
Kamera	Toiset kamerat, lasertutka, tutkat

Taulukosta havaitaan, että ajoneuvon toiminnan kannalta keskeisimmät yksittäiset tietokonenäön käyttämät komponentit ovat aina korvattavissa vaihtoehtoisilla laitteilla. Kirjallisuuskatsauksessa käytetyissä tutkimuksissa ei ole pystytty osoittamaan, että olisi käytännöllisesti mahdollista häiritä autonomisen ajoneuvon kaikkia keskeisimpiä komponentteja samaan aikaan siten, että auto ei pystyisi havaitsemaan ympäristöään yhdenkään laitteen avulla. Toisaalta myös tällaisen hypoteettisen tilanteen havainnointi ja tunnistaminen ovat tietoturvan kannalta keskeistä, sillä esimerkiksi mahdollisen kuljettajan varoittaminen tai pysäköinti tien sivuun saattaisi pelastaa ajoneuvon onnettomuudelta.

Kesäkuussa 2016 Teslan Autopilot-toimintoa käyttänyt yhdysvaltalaismies kuoli liikenneonnettomuudessa (Solomon 2016). Vaikkakin kuljettaja uutisen mukaan laiminlöi ajoneuvon varoitukset huomion kiinnittämisestä muuhun liikenteeseen, oli kyseessä ensimmäinen itseohjautuvan ajoneuvon kyydissä kuollut ihminen. Kyseinen onnettomuus on esimerkki siitä, millaisia riskejä huonosti toteutettu tietokonenäön sensorifuusio voi saada aikaan: perinpohjaisen tutkimuksen jälkeen selvisi, että järjestelmän kamera ei ollut sääolosuhteiden takia huomannut ajoneuvon edessä olevaa ajoneuvoa (Oremus 2016). Järjestelmä oli lähteen mukaan ohjelmoitu siten, että kamera oli aina tietokonenäön ensisijainen havainnointilaite, eikä toimenpiteitä tehty pelkästään tutkan saaman datan perusteella. Kuolemantapauksen jälkeen Autopilot-järjestelmän tehtiin muutos, jonka johdosta ajoneuvo pystyy toimimaan kameran lisäksi myös tutkan havaintojen perusteella.

Edistynyt sensorifuusio luonnollisesti edellyttää lukuisia erilaisia teknologioita tietokonenäön käytettäväksi, jotta itse fuusio on mahdollista. Teslan toimitusjohtaja Elon Muskin mukaan korkeimman tason autonominen ajoneuvo on toteutettavissa pelkästään eteenpäin suunnatun tutkan, kahdeksan videokameran sekä ultraääniantureiden avulla, eikä Teslan ajoneuvoissa tästä syystä ole käytetty lasertutkaa ollenkaan (Abuelsamid 2016; Tesla 2017). Toisten asiantuntijoiden mielestä lasertutka on muiden komponenttien ohella täysin välttämätön täyden autonomisuuden saavuttamiseksi (Kite-Powell 2017). Vain aika näyttää tarkemmin, millaisten teknologioiden ja apulaitteiden yhdistelmänä autonomisten ajoneuvojen tietokonenäkö saa toteutettua sensorifuusion tarpeeksi turvallisella tavalla.

6. YHTEENVETO JA JATKOTUTKIMUSTARPEET

Itseohjautuvat ajoneuvot tekevät kovaa vauhtia tuloaan markkinoille. Autonomisuuteen liittyvää teknologiaa on tutkittu yliopistojen ja erilaisten tutkimuslaitosten toimesta jo pitkään, ja viimeisen kymmenen vuoden aikana suuret ajoneuvovalmistajat ja teknologiajätit ovat lähteneet kehitystyöhön ja kaupallisten autonomisten autojen suunnitteluun mukaan. Ajoneuvovalmistajat lupailevat omia itseohjautuvia autojaan julkaistavan markkinoille vuosien 2017 ja 2022 välillä, joten teknologian kehityksen voi olettaa jatkuvan ripeänä myös lähitulevaisuudessa. SAE:n itseohjautuvuuden standardin mukaisen viidennen tason ajoneuvolla olisi valtava vaikutus liikenteeseen ja logistiikkaan, vaikuttaen potentiaalisesti mm. liikenneturvallisuuteen, kuljetuskustannuksiin, teiden ruuhkautumiseen ja käyttöasteeseen, liikenteestä aiheutuviin päästöihin sekä ihmisten liikkuvuuden helppouteen (Krasniqi & Hajrizi 2016).

Lähteen Krzanich (2016) mukaan yksittäinen autonominen ajoneuvo tulee tietokonenäkönsä toiminnan edellyttämänä vuonna 2020 keräämään ympäristöstään mm. lasertutkien ja lukuisten videokameroiden avulla n. 4 000 gigatavua dataa päivässä. Korkea datamäärä ennustaa autonomisesta liikennejärjestelmästämme entistä tietointensiivisempää, jolloin luonnollisesti myös tietoturvan rooli tulee liikenteessä kasvamaan. Ajoneuvovalmistajien on tuotteita suunnitellessaan osattava varautua siihen, että autojen tietokonenäön hyödyntämiin apulaitteisiin saattaa kohdistua tässä työssä esiteltyjen menetelmien kaltaisia tietoturvauhkia. Uhat saattavat toisinaan käydä toteen johtuen aktiivisesta ja pahansuovasta hyökkääjästä, tai sattuman kaupalla syntyneistä olosuhteista jotka saattavat häiritä tietokoneen tarvitsemaa komponenttia. Riippumatta tavasta jolla tietoturvauhka realisoituu, on tietokoneen osattava paitsi havaita mahdollinen uhka tai hyökkäys, myös käyttää tarpeeksi edistynyttä sensorifuusiota tietokonenäön saatavuuden ja oikeellisuuden ylläpitämiseksi ja toimenpiteiden tekemiseksi.

Työssä käytiin läpi autonomisen ajoneuvon tietokonenäön käyttämien komponenttien tekniset taustat, taulukoitiin näihin kohdistuvia tietoturvauhkia sekä esiteltiin menetelmiä, joilla kyseisiltä tietoturvauhilta on mahdollista puolustautua. Tietoa ja tutkimuksia oli saatavilla hyvin, joskin alan teknologia on kehittynyt niin nopeasti viimeisen kahden vuoden aikana, että jo vuosien 2015 tutkimukset saattoivat olla ristiriidassa ajankohtaisempien teknologiauutisten kanssa. Tutkimuksen avulla pystyttiin kuitenkin vastaamaan asetettuun päätutkimuskysymykseen, eli siihen, kuinka autonomisen ajoneuvon tietokonenäköön kohdistuvilta tietoturvahyökkäyksiltä voidaan puolustautua. Tietoa eri ajoneuvovalmistajien tietokonenäköön liittyvistä teknisistä toteutuksista oli saatavilla vielä suhteellisen niukasti, johtuen osittain siitä, että kaikki valmistajat eivät ole toistaiseksi julkaisseet omia autonomisia ajoneuvojaan julkisuuteen.

Yhdysvaltalaista ajoneuvovalmistaja Teslaa käytettiin tutkimuksessa suhteellisen paljon käytännön esimerkkinä, sillä yrityksen itseohjautuvaa Autopilot-järjestelmää on tutkimuksen hetkellä testattu todellisessa ajossa jo satojen miljoonien kilometrien verran (Solomon 2016). Yrityksen kirkkaiden tulevaisuuden visioiden sekä äänekkäiden lupausten johdosta Teslaa pidetään yhtenä itseohjautuvien ajoneuvojen kehittämisen edelläkävijöistä. Huomionarvoista kuitenkin on, että tutkimuksessa viitattu kuolemantapaus liittyen huonosti toteutettuun sensorifuusioon olisi voinut sattua mille tahansa muulle ajoneuvovalmistajalle, joka olisi vain sattunut olemaan ensimmäisten joukossa oman itseohjautuvan ajoneuvonsa julkaisun kanssa.

Mahdollisena jatkotutkimuksena tietokonenäön tietoturvaan liittyen olisi mielenkiintoista saada selville, kuinka haastavaa olisi häiritä autonomisen ajoneuvon käyttämistä komponenteista kahta tai useampaa samanaikaisesti, ja kuinka ajoneuvon tietokoneen tulisi reagoida tällaiseen tilanteeseen. Ala on kuitenkin tällä hetkellä erittäin nopeasti kehittyvässä trendissä, joten tietoturva saattaa helposti jäädä tulevaisuuden visioiden varjossa takaa-alalle. Toisaalta alalla riittää tietoturvan suhteen myös paljon muuta tutkittavaa, sillä tietokonenäkö on kokonaisuuden kannalta vain yksi osa itseohjautuvan ajoneuvon tietoturvaa: myös esimerkiksi langaton tiedonsiirto toisten ajoneuvojen kesken on yksi monista älyliikenteen kaavailluista sovelluksista. Langaton tiedonsiirto paitsi mahdollistaisi älykkäämmän ruuhkien ja tilannetietoisuuden hallinnan, myös avaisi monia ovia uusille tutkimusta vaativille tietoturvariskeille autonomisessa liikenteessä.

LÄHTEET

Abuelsamid, S. (2016). Tesla Autopilot Fatality Shows Why Lidar And V2V Will Be Necessary For Autonomous Cars. Forbes. 1.7.2016. Saatavilla: https://www.forbes.com/sites/samabuelsamid/2016/07/01/first-tesla-autopilot-fatality-demonstrates-why-lidar-and-v2v-probably-will-be-necessary/.

Ahuja, N. (2014). Computer vision. McGraw-Hill Education. 2014. Saatavilla: http://www.accessscience.com.libproxy.tut.fi/content/154050.

Anderson, J.M. (2003). Why we need a new definition of information security, Computers & Security, Vol. 22(4), pp. 308-313.

Ashley, S. (2016). Centimeter-accurate GPS for self-driving vehicles. 2.11.2016. Saatavilla: http://articles.sae.org/15067/.

Axelrod, C.W. (2017). Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks, 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), IEEE, pp. 1-6.

BBC News (2010). How computers took over our cars. 11.2.2010. Saatavilla: http://news.bbc.co.uk/2/hi/uk_news/magazine/8510228.stm.

Belvedere, M.J. (2017). Ford aims for self-driving car with no gas pedal, no steering wheel in 5 years, CEO says. 9.1.2017. Saatavilla: https://www.cnbc.com/2017/01/09/ford-aims-for-self-driving-car-with-no-gas-pedal-no-steering-wheel-in-5-years-ceo-says.html.

Bradbury, D. (2016). How Autonomous Vehicles Will Navigate Bad Weather Remains Foggy. Forbes. 29.11.2016. Saatavilla: https://www.forbes.com/sites/centurylink/2016/11/29/how-autonomous-vehicles-will-navigate-bad-weather-remains-foggy/.

Bridges, A. (2015). Explainer: What are lidar, radar and sonar? Science News for Students. 1.5.2015. Saatavilla: https://www.sciencenewsforstudents.org/article/explainer-what-are-lidar-radar-and-sonar.

Brooke, L. (2016). U.S. DoT chooses SAE J3016 for vehicle-autonomy policy guidance. SAE International. 20.9.2016. Saatavilla: http://articles.sae.org/15021/.

Broughton, J. & Baughan, C. (2002). The effectiveness of antilock braking systems in reducing accidents in Great Britain, Accident Analysis and Prevention, Vol. 34(3), pp. 347-355.

Cameron, O. (2017). An Introduction to LIDAR: The Key Self-Driving Car Sensor. Voyage. 9.5.2017. Saatavilla: https://news.voyage.auto/an-introduction-to-lidar-the-key-self-driving-car-sensor-a7e405590cff.

Caruso, R. (2017). In 1925 they already spoke about autonomous cars. Auto & Technica. 22.6.2017. Saatavilla: http://autoetecnica.band.uol.com.br/em-1925-ja-se-falava-em-carro-autonomo/.

CB Insights (2017). 44 Corporations Working On Autonomous Vehicles. 18.5.2017. Saatavilla: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/.

Chien, Y. (2015). Design of GPS Anti-Jamming Systems Using Adaptive Notch Filters, IEEE Systems Journal, Vol. 9(2), pp. 451-460.

Estl, H. (2016). Sensor fusion: A critical step on the road to autonomous vehicles. eeNews. 11.4.2017. Saatavilla: http://www.eenewseurope.com/news/sensor-fusion-critical-step-road-autonomous-vehicles.

Fox-Brewster, T. (2016). How to Crash a Self-Driving Car. Forbes. 4.8.2016. Saatavilla: https://www.forbes.com/sites/thomasbrewster/2016/08/04/tesla-autopilot-hack-crash/.

Gora, P. & Rüb, I. (2016). Traffic Models for Self-driving Connected Cars, Transportation Research Procedia, pp. 2207-2216.

Greene, K. (2006). Lights, Camera -- Jamming. MIT Technology Review. 22.6.2006. Saatavilla: https://www.technologyreview.com/s/405968/lights-camera-jamming/.

Hawes, N. (2016). Driving the revolution. University of Birmingham, The Birmingham Brief. 3.11.2016. Saatavilla: https://www.birmingham.ac.uk/news/thebirmingham-brief/items/2016/11/driving-the-revolution.aspx.

Hocheol, S., Dohyun, K., Yujin, K. & Yongdae, K. (2017). Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications. Korea Advanced Institute of Science and Technology, Dajeon, Republic of Korea. Saatavilla: https://eprint.iacr.org/2017/613.pdf.

International Organiation for Standardization (2016). ISO/IEC 27000:2016. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Saatavilla: https://www.iso.org/standard/66435.html.

J. Petit & S. E. Shladover (2015). Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems, Vol. 16(2), pp. 546-556.

Kim, G., Eom, J. & Park, Y. (2015). Investigation on the occurrence of mutual interference between pulsed terrestrial LIDAR scanners, The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings. Piscataway, pp. 437.

Kite-Powell, J. (2017). How To Make Autonomous Cars See Better. Forbes. 11.9.2017. Saatavilla: https://www.forbes.com/sites/jenniferhicks/2017/09/11/how-to-make-autonomous-cars-see-better/.

Krasniqi, X. & Hajrizi, E. (2016). Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles, IFAC-PapersOnLine, Vol. 49(29), pp. 269-274.

Krzanich, B. (2016). Data is the New Oil in the Future of Automated Driving. Intel Newsroom. 15.11.2017. Saatavilla: https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/.

Laugier, C., Paromtchik, I. & Parent, M. (1999). Developing autonomous maneuvering capabilities for future cars, Proceedings 199 IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems (Cat. No.99TH8383), pp. 68-73.

Mahafza, B. (1998). Introduction to Radar Analysis. CRC Press.

Meikle, H. (2008). Modern Radar Systems, 2; 2nd ed. Artech House Books, Norwood.

Mozur, P., Scott, M. & Frenkel, S. (2017). Mystery of Motive for a Ransomware Attack: Money, Mayhem or a Message? The New York Times. 28.6.2017. Saatavilla: https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html.

Muoio, D. (2017). RANKED: The 18 companies most likely to get self-driving cars on the road first. Business Insider. 3.4.2017. Saatavilla: http://nordic.businessinsider.com/the-companies-most-likely-to-get-driverless-cars-on-the-road-first-2017-4.

National Oceanic and Atmospheric Administation (2005). Do you know where you are? - The Global Positioning System, National Oceanic and Atmospheric Administation. Viitattu 21.10.2017. Saatavilla: https://oceanservice.noaa.gov/education/kits/geodesy/geo09_gps.html.

Nvidia (2017). The AI Car Computer For Autonomous Driving. Viitattu 11.10.2017. Saatavilla: https://www.nvidia.com/en-us/self-driving-cars/drive-px/.

Oagana, A. (2016). A Short History of Mercedes-Benz Autonomous Driving Technology, https://www.autoevolution.com/news/a-short-history-of-mercedes-benz-autonomous-driving-technology-68148.html.

Oremus, W. (2016). How Tesla Fixed a Deadly Flaw in Its Autopilot. Slate. 12.9.2016. Saatavilla: http://www.slate.com/articles/technology/future_tense/2016/09/how_tesla_s_software_update_fixed_a_deadly_flaw_in_autopilot.html.

Organisation Internationale des Constructeurs d'Automobiles (2016). World Motor Vehicle Production. Viitattu 17.10.2017. Saatavilla: http://www.oica.net/wp-content/uploads//ranking2015.pdf.

OxTS (2016). Why it is necessary to integrate an inertial measurement unit with imaging systems on an autonomous vehicle. Viitattu 19.10.2017. Saatavilla:

http://www.oxts.com/technical-notes/why-it-is-necessary-to-integrate-an-inertial-measurement-unit-with-imaging-systems-on-an-autonomous-vehicle/.

Panetta, K. (2017). Top Trends in the Gartner Hype Cycle for Emerging Technologies. Gartner. 15.8.2017. Saatavilla: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/.

Quain, J.R. (2017). What Self-Driving Cars See. The New York Times. 25.5.2017. Saatavilla: https://www.nytimes.com/2017/05/25/automobiles/wheels/lidar-self-driving-cars.html.

Reid, R. & Gilbert, A. (2010). Using the Parkerian Hexad to introduce security in an information literacy class, 2010 Information Security Curriculum Development Conference, ACM, pp. 45-47.

Roy, N., Hassanieh, H. & Choudhury, R.R. (2017). BackDoor: Making Microphones Hear Inaudible Sounds. Viitattu 27.10.2017. Saatavilla: http://synrg.csl.illinois.edu/papers/backdoor_mobisys17.pdf.

Santo, D. (2016). Autonomous Cars' Pick: Camera, Radar, Lidar? EE Times. 7.7.2016. Saatavilla: https://www.eetimes.com/author.asp?section_id=36&doc_id=1330069.

Society of Automotive Engineers (2016). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Viitattu 27.9.2017. Saatavilla: http://standards.sae.org/j3016_201609/.

Solomon, B. (2016). Tesla Autopilot Enthusiast Killed In First Self-Driving Car Death. Forbes. 30.6.2016. Saatavilla: https://www.forbes.com/sites/briansolomon/2016/06/30/the-first-self-driving-car-death-launches-tesla-investigation/#603475a37762.

Solon, O. (2016). Team of hackers take remote control of Tesla Model S from 12 miles away. The Guardian. 20.9.2016. Saatavilla: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes.

Straub, J., McMillan, J., Yaniero, B., Schumacher, M., Almosalami, A., Boatey, K. & Hartman, J. (2017). CyberSecurity considerations for an interconnected self-driving car system of systems, 2017 12th System of Systems Engineering Conference. SoSE 2017,

Taylor, M. (2017). The Level 3 Audi A8 Will Almost Be The Most Important Car In The World. Forbes. 10.9.2017. https://www.forbes.com/sites/michaeltaylor/2017/09/10/tthe-level-3-audi-a8-will-almost-be-the-most-important-car-in-the-world/#3a760730fb3d.

Tesla (2017). Tesla Autopilot. Viitattu 15.10.2017. Saatavilla: https://www.tesla.com/fi_FI/autopilot.

U.S. Department of Transportation (2015). Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey. Saatavilla: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115.

University of Texas (2013). UT Austin Researchers Spoof Superyacht at Sea. Cockrell School of Engineering. 29.7.2013. Saatavilla: http://www.engr.utexas.edu/features/superyacht-gps-spoofing.

Wojdyla, B. (2012). How it Works: The Computer Inside Your Car. Popular Mechanics. 21.2.2012. Saatavilla: http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/.

Wong, J.I. (2016). Driverless cars have a new way to navigate in rain or snow. Quartz. 14.3.2016. Saatavilla: https://qz.com/637509/driverless-cars-have-a-new-way-to-navigate-in-rain-or-snow/.

World Health Organization (2017). Road traffic injuries, Fact sheet. Viitattu 12.10.2017. Saatavilla: http://www.who.int/mediacentre/factsheets/fs358/en/.

World Health Organization (2004). World report on road traffic injury prevention. Viitattu 12.10.2017. Saatavilla: http://apps.who.int/iris/bitstream/10665/42871/1/9241562609.pdf.

Yağdereli, E., Gemci, C. & Aktaş, A.Z. (2015). A study on cyber-security of autonomous and unmanned vehicles, The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 12(4), pp. 369-381.

Zhang, Z., Trinkle, M., Qian, L. & Li, H. (2012). Quickest detection of GPS spoofing attack, MILCOM 2012 - 2012 IEEE Military Communications Conference, IEEE, pp. 1-6.